МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»»

ЛАБОРАТОРНАЯ РАБОТА №2:
«Анализ дампа трафика протокола Modbus»

По предмету Информационная безопасность АСУ ТП

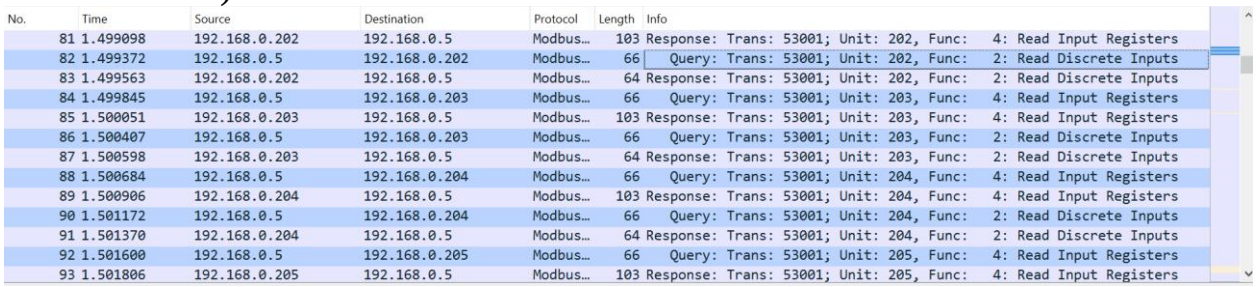
Выполнила студентка группы Б19-515
Щербакова Александра

Москва, 2022 г.

Задание 1.

Используя дамп трафика, определить, какие из устройств являются slave, а какое – master.

Предоставленный дамп трафика открыт в Wireshark. Можно заметить, что отправляет запросы только устройство с IP 192.168.0.5. Остальные устройства отвечают на эти запросы. Это соответствует схеме работы протокола Modbus – одно устройство является master-устройством (в данном случае это 192.168.0.5), а все остальные – slave (192.168.0.201 – 192.168.0.205).

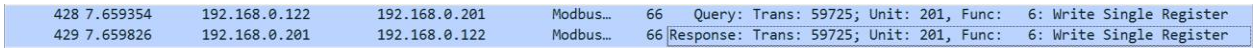


No.	Time	Source	Destination	Protocol	Length	Info
81	1.499098	192.168.0.202	192.168.0.5	Modbus…	103	Response: Trans: 53001; Unit: 202, Func: 4: Read Input Registers
82	1.499372	192.168.0.5	192.168.0.202	Modbus…	66	Query: Trans: 53001; Unit: 202, Func: 2: Read Discrete Inputs
83	1.499563	192.168.0.202	192.168.0.5	Modbus…	64	Response: Trans: 53001; Unit: 202, Func: 2: Read Discrete Inputs
84	1.499845	192.168.0.5	192.168.0.203	Modbus…	66	Query: Trans: 53001; Unit: 203, Func: 4: Read Input Registers
85	1.500051	192.168.0.203	192.168.0.5	Modbus…	103	Response: Trans: 53001; Unit: 203, Func: 4: Read Input Registers
86	1.500407	192.168.0.5	192.168.0.203	Modbus…	66	Query: Trans: 53001; Unit: 203, Func: 2: Read Discrete Inputs
87	1.500598	192.168.0.203	192.168.0.5	Modbus…	64	Response: Trans: 53001; Unit: 203, Func: 2: Read Discrete Inputs
88	1.500684	192.168.0.5	192.168.0.204	Modbus…	66	Query: Trans: 53001; Unit: 204, Func: 4: Read Input Registers
89	1.500906	192.168.0.204	192.168.0.5	Modbus…	103	Response: Trans: 53001; Unit: 204, Func: 4: Read Input Registers
90	1.501172	192.168.0.5	192.168.0.204	Modbus…	66	Query: Trans: 53001; Unit: 204, Func: 2: Read Discrete Inputs
91	1.501370	192.168.0.204	192.168.0.5	Modbus…	64	Response: Trans: 53001; Unit: 204, Func: 2: Read Discrete Inputs
92	1.501600	192.168.0.5	192.168.0.205	Modbus…	66	Query: Trans: 53001; Unit: 205, Func: 4: Read Input Registers
93	1.501806	192.168.0.205	192.168.0.5	Modbus…	103	Response: Trans: 53001; Unit: 205, Func: 4: Read Input Registers

Задание 2.

В дампе трафика присутствует только одна пара запрос-ответ на запись регистров, в то время как остальные – только на чтение. Найти данную пару.

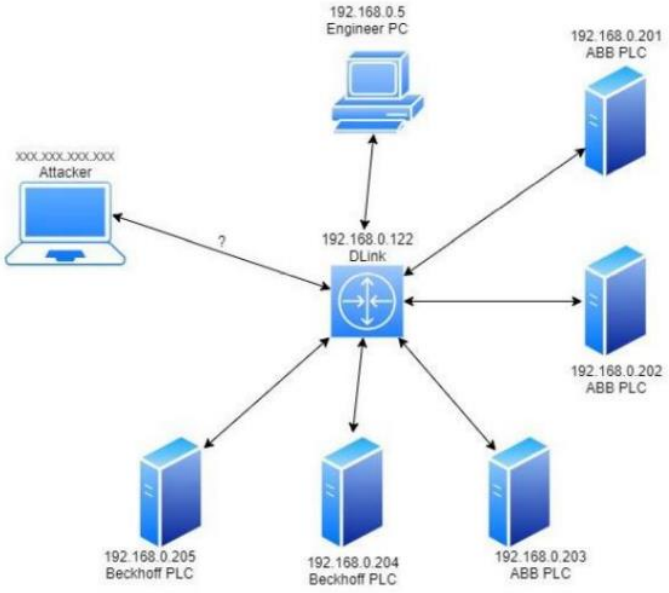
По условию задания подходит только функция Write Single Register (запись в регистр).



428	7.659354	192.168.0.122	192.168.0.201	Modbus…	66	Query: Trans: 59725; Unit: 201, Func: 6: Write Single Register
429	7.659826	192.168.0.201	192.168.0.122	Modbus…	66	Response: Trans: 59725; Unit: 201, Func: 6: Write Single Register

Задание 3.

Используя карту топологии сети, определить, происходило ли вторжение в сеть на момент записи трафика.



Можно заметить, что IP 192.168.0.50 нет на схеме топологии сети. Тем не менее, запрос с этого устройства проведен, значит, это злоумышленник.

```
531 9.505025    192.168.0.50    192.168.0.205    Modbus…    66    Query: Trans: 57097; Unit: 205, Func:   2: Read Discrete Inputs
```

Вызвана функция Read Decrease Inputs:

```
> Frame 531: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF
> Ethernet II, Src: Apple_b3:fa:78 (00:11:24:b3:fa:78), Dst: Beckhoff_23:60:54 (00:01:05:23:60:
> Internet Protocol Version 4, Src: 192.168.0.50, Dst: 192.168.0.205
> Transmission Control Protocol, Src Port: 49467, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
> Modbus/TCP
v Modbus
    .000 0010 = Function Code: Read Discrete Inputs (2)
    Reference Number: 0
    Bit Count: 2
```

```
0000  00 01 05 23 60 54 00 11  24 b3 fa 78 08 00 45 00   ···#`T·· $··x··E·
0010  00 34 50 37 40 00 80 06  28 6a c0 a8 00 32 c0 a8   ·4P7@··· (j···2··
0020  00 cd c1 3b 01 f6 6c a9  34 7b 23 c1 98 34 50 18   ···;··l· 4{#··4P·
0030  01 00 60 3d 00 00 df 09  00 00 00 06 cd 02 00 00   ··`=···· ········
0040  00 02                                             ··
```

Ответ на запрос:

```
532 9.505214    192.168.0.205    192.168.0.50    Modbus/T…    64 Response: Trans: 57097; Unit: 205, Func:   2: Read Discrete Inputs
```

```
> Frame 532: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF
> Ethernet II, Src: Beckhoff_23:60:54 (00:01:05:23:60:54), Dst: VMware_8d:19:54 (00:0c:29:8d:19
> Internet Protocol Version 4, Src: 192.168.0.205, Dst: 192.168.0.50
> Transmission Control Protocol, Src Port: 502, Dst Port: 49467, Seq: 1, Ack: 13, Len: 10
> Modbus/TCP
v Modbus
    .000 0010 = Function Code: Read Discrete Inputs (2)
    [Request Frame: 531]
    [Time from request: 0.000189000 seconds]
    Byte Count: 1
  > Bit 0 : 1
  > Bit 1 : 0
```

```
0000  00 0c 29 8d 19 54 00 01  05 23 60 54 08 00 45 00   ··)··T·· ·#`T··E·
0010  00 32 69 ee 40 00 80 06  0e b5 c0 a8 00 cd c0 a8   ·2i·@··· ········
0020  00 32 01 f6 c1 3b 23 c1  98 34 6c a9 34 87 50 18   ·2···;#· ·4l·4·P·
0030  00 fe 5f 38 00 00 df 09  00 00 00 04 cd 02 01 01   ··_8···· ········
```